

Complete if Known

Application Number	10/765,976
Filing Date	January 29, 2004
First Named Inventor	VANSTONE
Art Unit	NOT YET SPECIFIED
Examiner Name	NOT YET SPECIFIED
Attorney Docket Number	T00001-0378-US1

(use as many sheets as necessary)

Sheet	1	of	2	Attorney Docket Number	T00001-0378-US1
-------	---	----	---	------------------------	-----------------

[illegible][illegible]

Date Considered

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449B/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 2 of 2

Complete if Known

Application Number	10/765,976
Filing Date	January 29, 2004
First Named Inventor	VANSTONE
Art Unit	NOT YET SPECIFIED
Examiner Name	NOT YET SPECIFIED
Attorney Docket Number	T00001-0378-US1

OTHER PRIOR ART -- NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No. ¹	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T ²
		KOBLITZ, "CM-Curves with Good Cryptographic Properties", Advances in Cryptology, Santa Barbara, Aug. 11-15, 1991, Proceedings of the Conference on Theory and Applications of Cryptographic Techniques, Berlin, Springer, DE, 1991, pages 279-287.	
		MEIER W ET AL, "Efficient Multiplication on Certain Nonsupersingular Elliptic Curves", Advances in Cryptology, Santa Barbara, Aug. 16-20, 1992, Proceedings of the Annual International Cryptology Conference, Berlin, Springer, DE, vol. CONF. 12, pages 333-344.	
		SCHOOF R, "Elliptic Curves over Finite Fields and the Computation of Square Roots Mod P", Mathematics of Computation, American Mathematical Society, US, vol. 44, no. 169/170, April 1985, pages 483-494.	
		LAY G-J ET AL, "Constructing Elliptic Curves with Given Group Order Over Large Finite Fields", Algorithmic Number Theory, International Symposium, 1994, pages 250-263.	
		MUELLER V, "Fast Multiplication on Elliptic Curves over Small Fields of Characteristic Two", PUBLICATIONS, TU DARMSTADT, 1997	
		SCHNEIER, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", 1994, pages 39-41, John Wiley & Sons, New York.	

Examiner
Signature

Date
Considered

2 JUL 05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not

¹ Applicant's unique citation designation number (optional). ² Applicant is to place a check mark here if English language Translation is attached. This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 120 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.